Notice of Allowability	Application No.	Applicant(s)	
	10/626,948	EISENTRAEGER ET AL.	
	Examiner	Art Unit	
	Samson B. Lemma	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *amendment filed on 02/20/2007,* .

2. ☒ The allowed claim(s) is/are *1, 4, 6-16, 20-28, 31-37, 46-47, 50, 53-57, 59-66, 68-70 and 72,* .

3. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a) ☐ All b) ☐ Some* c) ☐ None of the:
      1. ☐ Certified copies of the priority documents have been received.
      2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
      3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
      1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
   (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☐ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. ☒ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date 03/12/2007
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application
6. ☒ Interview Summary (PTO-413), Paper No./Mail Date *03/12/2007* .
7. ☒ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____.

DETAILED ACTION

1. This is in reply to amendment after non-final office action, filed on February 20, 2007. **Claims 2-3, 5, 17-19, 29-30, 39, 43, 48-49, 51-52, 58, 67 and 71,** are originally canceled. No new claims are added.

2. Claims **1, 4, 6-8, 11, 14, 16, 20, 26, 27, 31-34, 37, 38, 40-41, 44, 47, 50, 53-56, 65, and 69** have been amended.

3. Before the examiner's amendment, there **are 12 independent claims** namely **1, 16, 27, 38, 47, 50, 53-56, 65 and 69. All of these** independent claims are amended.

EXAMINER'S AMENDMENT

An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview **with Shirley Lee Anderson (Registration No. 57,763) on 03/12/2007.**

The application has been amended as follows: In the claims

16. (Currently amended) In claim 16, line 1, please delete, "computer-readable medium", and replace it with, "computer storage media".

20. (Currently amended) In claim 20, line 1, please delete "computer-readable medium", and replace it with, "computer storage media".

21. (Currently amended) In claim 21, line 1, please delete "computer-readable medium", and replace it with, "computer storage media".

22. (Currently amended) In claim 22, line 1, please delete "computer-readable medium", and replace it with, "computer storage media".

23. (Currently amended) In claim 23, line 1, please delete "computer-readable medium", and replace it with, "computer storage media".

24. (Currently amended) In claim 24, line 1, please delete "computer-readable medium", and replace it with, "computer storage media".

25. (Currently amended) In claim 25, line 1, please delete "computer-readable medium", and replace it with, "computer storage media".

26. (Currently amended) In claim 26, line 1, please delete "computer-readable medium", and replace it with, "computer storage media".

38. (Canceled)

40. (Canceled)

41. (Canceled)

42. (Canceled)

44. (Canceled)

45. (Canceled)

47. (Currently amended) In claim 47, line 1, please delete, "computer-readable medium" and replace it, "computer storage media".

54. (Currently amended) In claim 54, line 1, please delete, "computer-readable medium" and replaces with, "computer storage media".

65. (Currently amended) In claim 65, line 1, please delete, "computer-readable medium" and replaces it with, "computer storage media".

66. (Currently amended) In claim 66, line 1, please delete "computer-readable medium", and replace it with, "computer storage media".

68. (Currently amended) In claim 68, line 1, please delete, "computer-readable medium" replace it with, the following limitation, "computer storage media".

Allowable Subject Matter

4. As the result of Examiner's amendment,

- Independent **claim 38** and the corresponding dependent claims **40-42 and 44-45** are canceled. These claims are found to be not allowable.
  Thus claims 1, 4, 6-16, 20-28, 31-37, 46-47, 50, 53-57, 59-66, 68-70 and 72 are pending/examined.

- Independent **claims 16, 47, 54 and 65** and the corresponding dependent claims **20-26, 66 and 68 are amended**. Such amendment is made to make these claims directed **to statutory subject matter.** According to the applicant specification (see on page 28, lines 10-25), the language of the claims recited in the indepenent claims 16, 47, 54 and 65 and the corresponding depenent claims are directed to non-statutory subject matter. This is because, the computer-readable medium, recited in these claims are defined in the specification as both "computer storage media" which is defined as statutory and "communication media" which is defined as non-statutory. In order to make the claims statutory, both parties (Examiner and Applicant's representative) agreed to replace the term, "**computer-readable medium**" with "**computer storage media**" in the respective claims. This will exclude the non-statutory "communication media" recited on page 28, lines 10-25 of the specification.

5. **Claims 1, 4, 6-16, 20-28, 31-37, 46-47, 50, 53-57, 59-66, 68-70 and 72** are allowed. After the examiner's amendment, there are now 11 independent

claims, namely, namely **1, 16, 27, 47, 50, 53-56, 65 and 69. All of these** independent claims are amended.

6. The following is an examiner's statement of reasons for allowance:

Except for the 101 rejections, independent claims 53-55 were previously allowed. Applicant's successfully overcomes the 101-rejection set forth in the previous office action for these independent claims.

Referring to **the independent claims 1, 16, 27, 47, 56, 65 and 69** the art on the record, namely **Boneh discloses a method comprising: selecting an elliptic curve; determining a Squared Weil pairing based on said elliptic curve; and cryptographically processing selected information based on said Squared Weil pairing**. [Abstract, paragraph 0331-0347, paragraph 0354-0357] (As it is disclosed on the abstract, According to one embodiment, the bilinear map is based on a **Weil pairing or a Tate pairing defined on a subgroup of an elliptic curve**. Furthermore on paragraph 0331-0347, how the weil pairing is computed is disclosed on paragraph 0354, "To evaluate the Weil pairing e(P, Q), how the **repeated squaring algorithm** needs evaluate a function is also disclosed.)

On the rest of the former independent claim, namely independent claim 50, the combination of the references namely **Boneh and Mano discloses most of the limitations recited on previous independent claims. For instance as per former independent claim 50, Boneh discloses, a method comprising: selecting an elliptic curve; determining a Squared Weil pairing based on said elliptic curve; and cryptographically processing selected information based on said Squared Weil pairing.** [Abstract, paragraph 0331-0347, paragraph 0354-0357] (As it is disclosed on the abstract, According to one embodiment, the bilinear map is based on a **Weil pairing or a Tate pairing defined on a subgroup of an elliptic curve**. Furthermore on paragraph 0331-

0347, how the weil pairing is computed is disclosed on paragraph 0354, "To evaluate the Weil pairing e(P, Q), how the **repeated squaring algorithm** needs evaluate a function is also disclosed.)

Boneh does not explicitly disclose determining/computing a Squared Weil Pairing $e_m(P, Q)^2$ by:

establishing an odd prime m on a curve E; and based on two m-torsion points P and Q on E.

However, in the same field of endeavor **Mano**, discloses

- establishing an odd prime m on a curve E; and based on two m-torsion points P and Q on E. [page 707, 1st paragraph, page 704, 2nd paragraph, last line and 3rd paragraph, under the title "A result of skinner and Wiles]

▶ **However after the independent claims are amended,** it is been found that some of the limitations are not explicitly suggested by the reference on the record, namely **Boneh or by the combination of the references, Boneh and Mano**.

None of the prior art of record taken singularly of in combination teaches or suggests a distinct method of determining a Squared Weil pairing based on the elliptic curve; and cryptographically processing selected information based on said Squared Well pairing. The examiner asserts that the limitation recited on the respective independent claims after amendment are novel.

For the reasons provided above, the amended independent claims **1, 16, 27, 47, 50, 53-56, 65 and 69** are allowed.

7. **The dependent claims which are dependent on the independent claims 1, 16, 27, 47, 50, 53-56, 65 and 69 respectively** being further limiting to the independent claims, definite and enabled by the specification are also allowed.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submission should be clearly labeled "Comments on Statement of Reasons for Allowance."

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Samson B Lemma whose telephone number is 571-272-3806. The examiner can normally be reached on Monday-Friday (8:00 am --4: 30 pm).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, BARRON JR GILBERTO can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

SAMSON LEMMA
S.L.
03/12/2007

GILBERTO BARRON JR
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100